TEOREMA CINESE DEI RESTI

Siano $n_1, n_2, \dots, n_r$ interi positivi
con $MCD(n_i, n_j) = 1$ per $i \neq j$
$1 \leq i, j \leq r$ e siano $b_1, b_2, \dots, b_r$ interi.
Allora il sistema

$$\begin{cases} x \equiv b_1 \bmod n_1 \\ x \equiv b_2 \bmod n_2 \\ \vdots \\ x \equiv b_r \bmod n_r \end{cases}$$

è risolvibile.
Se c e $\bar{c}$ sono due soluzioni del sistema, allora $c \equiv \bar{c} \bmod N$,
dove $N = n_1 \cdots n_r$

$N_i = N/n_i$ per $i = 1 \dots r$
$MCD(N_i, n_i) = 1$
$N_i y \equiv 1 \bmod n_i$
y_i una soluzione
$c = \sum_i N_i y_i b_i$

ESEMPIO

1. Risolvere in $\mathbb{Z}$ il sistema

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 5 \\ x \equiv 2 \bmod 7 \end{cases}$$

Sol. $N = 3 \cdot 5 \cdot 7 = 105$
$N_1 = N/n_1 = 35$
$N_2 = N/n_2 = 3 \cdot 7 = 21$
$N_3 = N/n_3 = 3 \cdot 5 = 15$

Risolvere $N_1 y \equiv 1 \bmod n_1$
$35 y \equiv 1 \bmod 3$
$2 y \equiv 1 \bmod 3$
$y_1 = 2$

Risolvere $N_2 y \equiv 1 \bmod n_2$
$21 y \equiv 1 \bmod 5$
$y \equiv 1 \bmod 5$
$y_2 = 1$

Risolvere $N_3 y \equiv 1 \bmod n_3$
$15 y \equiv 1 \bmod 7$
$y \equiv 1 \bmod 7$
$y_3 = 1$

Una soluzione del sistema è
$c = \sum_1^3 N_i y_i b_i = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2$
$= 140 + 63 + 30 = 233$
Tutte le soluzioni sono
$c = 233 + k105 = 23 + k105$ al variare di $k \in \mathbb{Z}$
23 è la più piccola soluzione intera positiva

2. Risolvere in $\mathbb{Z}$ il sistema

$$\begin{cases} x \equiv 3 \mod 21 \\ x \equiv 5 \mod 16 \\ x \equiv 17 \mod 25 \end{cases}$$

$N = 21 \cdot 16 \cdot 25 = 8400$
$N_1 = N/m_1 = 16 \cdot 25 = 400$
$N_2 = N/m_2 = 21 \cdot 25 = 105 + 420 = 525$
$N_3 = N/m_3 = 21 \cdot 16 = 336$

Risolvere $N_1 y \equiv 1 \mod m_1$ cioè $400\,y \equiv 1 \mod 21$
ovvero $y \equiv 1 \mod 21$. Trovo $y_1 = 1$
$N_2 y \equiv 1 \mod m_2$ cioè $525\,y \equiv 1 \mod 16$
ovvero $13y \equiv 1 \mod 16$
$s, t \in \mathbb{Z}$ $13s + 16t = 1$

$16 = 13 \cdot 1 + 3$
$13 = 3 \cdot 4 + 1$
$3 = 1 \cdot 3 + 0$

$3 = 16 - 1 \cdot 13$
$1 = 13 - 3 \cdot 4 = 13 - (16 - 13) \cdot 4 = 5 \cdot 13 - 4 \cdot 16$

Una soluzione della congruenza
$y_2 = 5$

Risolvere $N_3 y \equiv 1 \mod m_3$ cioè
$336\,y \equiv 1 \mod 25$
$11\,y \equiv 1 \mod 25$

$25 = 11 \cdot 2 + 3$
$11 = 3 \cdot 3 + 2$
$3 = 2 \cdot 1 + 1$
$2 = 2 \cdot 1$

$3 = 25 - 2 \cdot 11$
$2 = 11 - 3 \cdot 3 = 11 - 3(25 - 2 \cdot 11)$
$1 = 3 - 2 = 7 \cdot 11 - 3 \cdot 25$
$1 = 25 - 2 \cdot 11 + (11 - 3 \cdot 3)$
$= 25 - 2 \cdot 11 + 7 \cdot 11 + 3 \cdot 25$
$= 4 \cdot 25 - 9 \cdot 11$

$y_3 = -9$. Una soluzione del sistema è

$$c = \sum_{i=1}^{3} N_i y_i b_i = 400 \cdot 1 \cdot 3 + 525 \cdot 5 \cdot 5 + 336 \cdot (-9) \cdot 17 =$$
$$= 1200 + \ldots = -37083$$

Tutte e sole le soluzioni sono
$-37083 + 8400k$ al variare di k in $\mathbb{Z}$
ovvero $4917 + 8400k$, al variare di k in $\mathbb{Z}$

Risolvere in $\mathbb{Z}$ il sistema

$$\begin{cases} 3x \equiv 2 \mod 5 \\ 5x \equiv 7 \mod 12 \\ 3x \equiv 1 \mod 7 \end{cases}$$

Considero $3x \equiv 2 \mod 5$. Allora 3 è invertibile modulo 5 con inverso 2.
Moltiplico la congruenza per 2 (= inverso di 3)
e trovo $x \equiv 4 \mod 5$

Considero $5x \equiv 7 \mod 12$: $MCD(5, 12) = 1$ quindi 5 è invertibile modulo 12 con inverso 5

$x \equiv 35 \mod 12$
e trovo $x \equiv 35 \mod 12$

$3x \equiv 1 \mod 7$: di nuovo moltiplico per 5 (= inverso di 3 modulo 7)
e trovo

$x \equiv 5 \mod 7$

$$\begin{cases} x \equiv 4 \bmod 5 \\ x \equiv 11 \bmod 12 \\ x \equiv 7 \bmod 7 \end{cases}$$

$N = 5 \cdot 12 \cdot 7 = 420$
$N_1 = N/m_1 = 12 \cdot 7 = 84$
$N_2 = N/m_2 = 5 \cdot 7 = 35$
$N_3 = N/m_3 = 5 \cdot 12 = 60$

1) $N_i x \equiv 1 \bmod m_i$
$84x \equiv 1 \bmod 5$
$4x \equiv 1 \bmod 5$
$y_1 = 4$

2) $35y \equiv 1 \bmod 12$
$-y \equiv 1 \bmod 12$
$y_2 = -1$

3) $60y \equiv 1 \bmod 7$
$4y \equiv 1 \bmod 7$
$y_3 = 2$

$$c = \sum_{i=1}^{3} N_i b_i y_i = 84 \cdot 4 \cdot 4 + 35 \cdot 11 \cdot (-1) + 60 \cdot 2 \cdot 7 = 385 + 840 = 1559$$

$1559 + 420k, \; k \in \mathbb{Z}$

$299 + 420k, \; k \in \mathbb{Z}$

ESEMPI
Risolvere in $\mathbb{Z}$ il sistema

$$\begin{cases} 3x \equiv 6 \bmod 18 \\ 3x \equiv 4 \bmod 5 \\ 2x \equiv 3 \bmod 7 \end{cases}$$

Consideriamo $3x \equiv 6 \bmod 18$. Ha soluzione se e solo se $MCD(3, 18) \mid 6$ ovvero se e solo se $3 \mid 6$. Allora $3x \equiv 6 \bmod 18$ equivale $x \equiv 2 \bmod 6$.

$$x \equiv \frac{a}{MCD(a,m)} \equiv \frac{b}{MCD(a,m)} \bmod \frac{m}{MCD(a,m)}$$

$$\begin{cases} x \equiv 2 \bmod 6 \\ x \equiv 3 \bmod 5 \\ x \equiv 5 \bmod 7 \end{cases}$$

$N = 6 \cdot 5 \cdot 7 = 210$
$N_1 = 35$
$N_2 = 42$
$N_3 = 30$

$35y \equiv 1 \bmod 6$
$5y \equiv 1 \bmod 6$
$y_1 = -1$

$42y \equiv 1 \bmod 5$
$2y \equiv 1 \bmod 5$
$y_2 = 3$

$30y \equiv 1 \bmod 7$
$2y \equiv 1 \bmod 7$
$y_3 = 4$

$$c = \sum_{i=1}^{3} N_i b_i y_i = 35 \cdot 2 \cdot (-1) + 42 \cdot 3 \cdot 3 + 30 \cdot 4 \cdot 5 = -70 + 600 = 308$$

Tutte e sole le soluzioni $c = 308 + k210 = 68 + k210, \; k \in \mathbb{Z}$